RSAC 2025 Conference

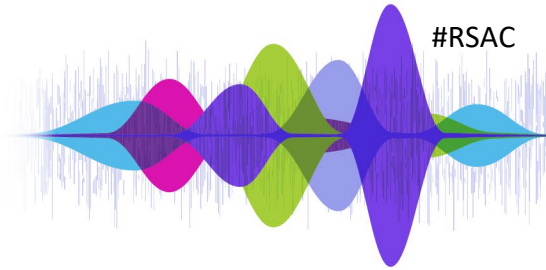
Many Voices.
One Community.

SESSION ID: APP-R01

The AppSec Playbook: Building World-Class Security from Scratch

David Kosorok

Director, Information Security Programs
Toast, Inc.
https://www.linkedin.com/in/kosorok/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

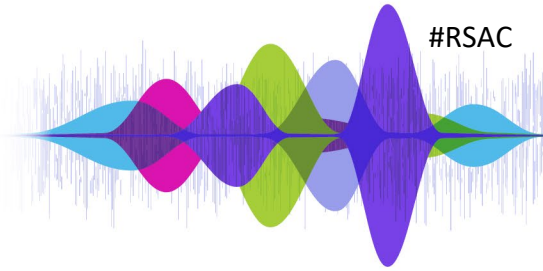
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The views and opinions expressed in this presentation are solely those of the speaker and do not necessarily reflect the official policy or position of Toast or any other affiliated entities.

Problem Story Time – The SQLi Incident

- Released high quality software.
- Within hours a SQLi was discovered and exploited.
- Code reviewed for quality, but not security.
- Risk appetite hadn’t been thought about.

Success Metric for this Session



By the end of this talk, you'll walk away with:

- A five-step playbook to assess and scale your AppSec program.
- How to prioritize security initiatives based on business impact.
- Key metrics to measure AppSec maturity and influence buy-in.

Fair Warning…

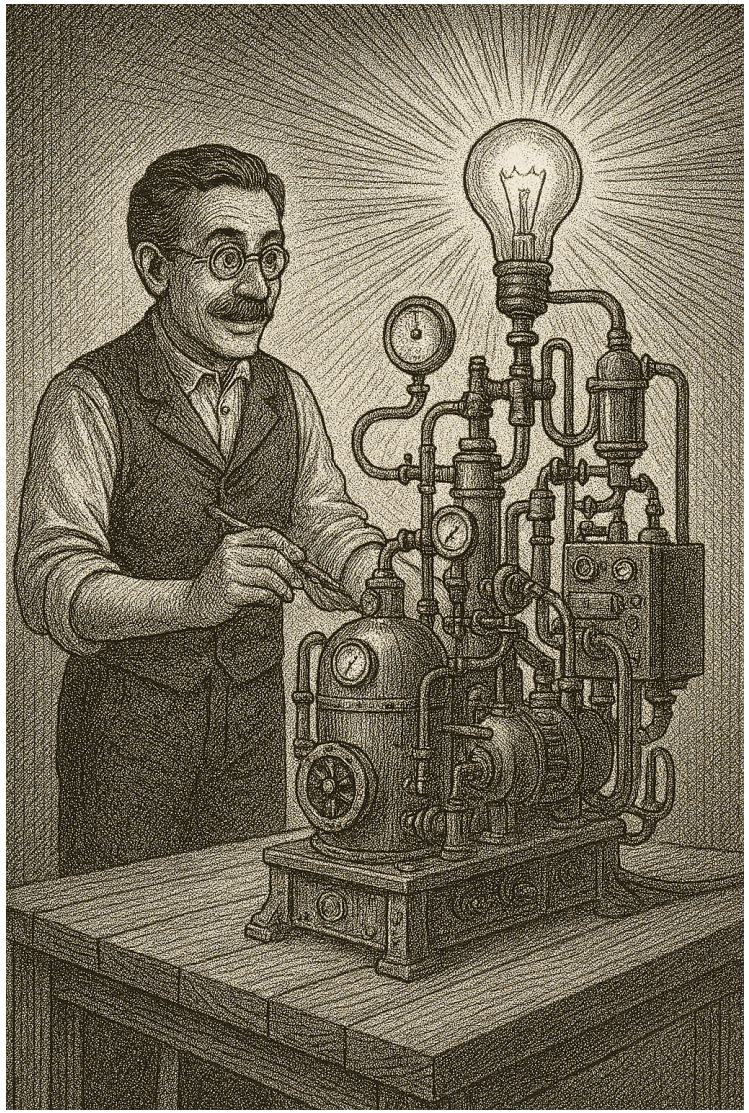
This presentation is:

- Based on nearly two decades of experience in security.
- From case studies presented here are drawn from past experience.
- Not proprietary or confidential.
- Intended to spark discussions and provide actionable insights.

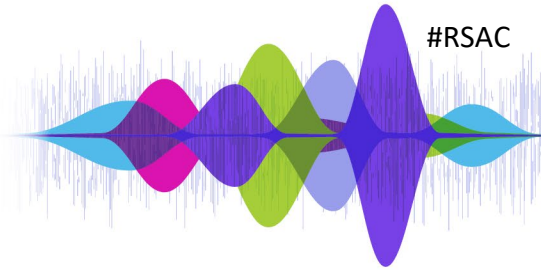
🚀 Let’s dive in!

Build an AppSec Playbook

- Interview Stakeholders
- Brainstorm Initiatives
- Assess State
- Prioritize with Risk Lens
- Measure

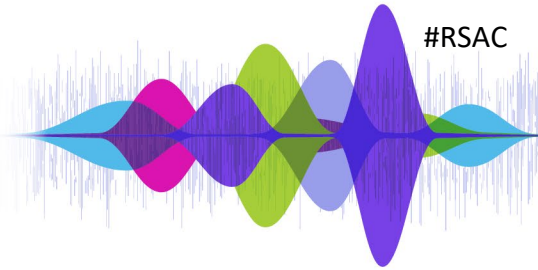


Step 1: Stakeholder Interviews



- Categorize responses into
  - Risk Areas
  - Business Pain Points
  - Cultural Gaps

Step 1: Stakeholder Interviews



Key questions to ask:

1. What keeps you up at night?
2. What's the impact of a security issue for you?
3. Does your team have adequate AppSec training?
4. Who else should I talk to?
5. Others…?

Step 2: Brainstorm Initiatives

- Predict
- Identify
- Prevent
- Detect
- Respond

Step 2: Brainstorm Initiatives

PREDICT	IDENTIFY	PREVENT		DETECT		RESPOND	
Threat Intelligence	M & A Security Playbook	Threat Modeling	AppSec Policies	SAST	SCA	Security SLA	Bug Bounty
AI Leveraging	NIST 800-53 Assessment	Security Champions	Team Self Development	DAST	MAST	External App Layer PenTests	PSIRT
Fraud Behavior	Internal Code Inventory	Metrics Dashboard	Security Architecture	Internal App PenTesting	Fuzzing	QA/AppSec Regression Testing	CTF Training
	ASVS Requirements	Dev Security Education	Vulnerability Guidelines	IAST	QA Partnership	Red Team Activities	Customer PenTests
	Asset Inventory	Vulnerability Remediation Education	Security Culture	CICD Integration	Validate 3rd Party APIs	WAF	Honey-potting
		Challenge Coin Award	Security Ambassadors	Container Scanning	Validate Partner Integrations	Typo-squatting Detection	Subdomain Validation
		Security Newsletter	Internal Security Summits	Security Test Code Coverage	Code Signing	Risk Acceptance	Reverse Engineering
		SSDLC Documentation	Monthly Brown Bags	Internal Security Toolkit	AppSecOps		
		QA Security Education	Enterprise Security Docs	Continuous Security Monitoring			
		Secure Coding Standards	Security Unit Tests				

Step 3: Assess Current State

NOT IMPLEMENTED = NI

IMPLEMENTED = I

OPERATIONAL = O

Step 4: Prioritize Initiatives

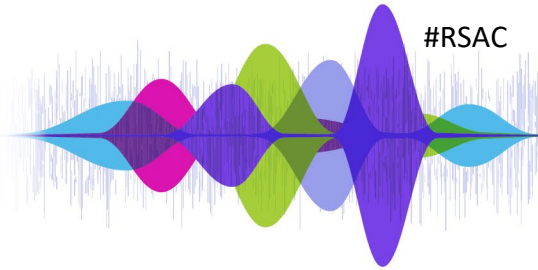
Priority	Initiatives	Primary Owner	Secondary Owner	Jira Epic	Effort	Current State	Year 1	Year 2	Year 3
1	Threat Intelligence	Gordon	Massimo		1 - Small	NI	O	O	O
2	M&A Security Playbook	Wolfgang			2 - Medium	I	I	O	O
3	Threat Modeling	Massimo			2 - Medium	I	I	O	O
4	AppSec Policies	Anne-Sophie			1 - Small	O	O	O	O
5	SAST	Thomas			3 - Large	NI	NI	O	O
6	SCA	Heston	David		5 - Extra Large	I	I	O	O
7	Security SLA	David			2 - Medium	I	I	O	O
8	Bug Bounty	Gordon			8 - Massive	NI	I	O	O
9	AI Leveraging	Wolfgang			5 - Extra Large	NI	NI	NI	NI
10	NIST 800-53 Assessment	Massimo			2 - Medium	NI	NI	O	O
11	Security Champions	Anne-Sophie	Gordon		5 - Extra Large	I	I	O	O
12	Team Self Development	Thomas			3 - Large	I	I	O	O
13	DAST	Heston			5 - Extra Large	NI	NI	I	I
14	MAST	David			2 - Medium	NI	O	O	O
15	External App Layer PenTests	Gordon			2 - Medium	NI	NI	O	O
16	PSIRT	Wolfgang			5 - Extra Large	NI	NI	I	I
17	Fraud Behavior	Massimo			5 - Extra Large	NI	NI	NI	NI

Step 4: Prioritize Initiatives

Things to think about when prioritizing:

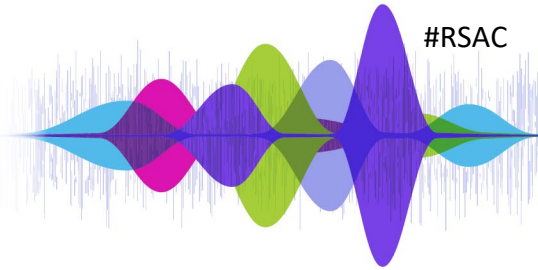
- **High Impact, Low Effort**
- **High Impact, High Effort**
- **Low Impact, High Effort**

Step 5: Measure, Own, Optimize



1. Be **on** the team.
2. Own **budgeting**, working with **procurement**.
3. Establish **goals** and **metrics** for each initiative.
4. Build, maintain and optimize the **implementation** plan.

Case Study #1 – The Beginning

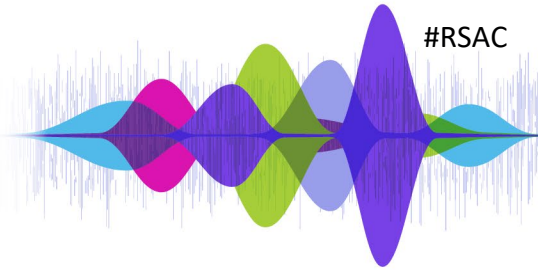


- **Challenge**:
  - No dedicated AppSec team.
  - High-quality software released without security reviews.
  - SQL injection (SQLi) vulnerability exploited post-release.
- **Business Risk Tolerance:**
  - Very low—but they didn't know it yet. The SQLi incident revealed it.

Case Study #1 – The Beginning

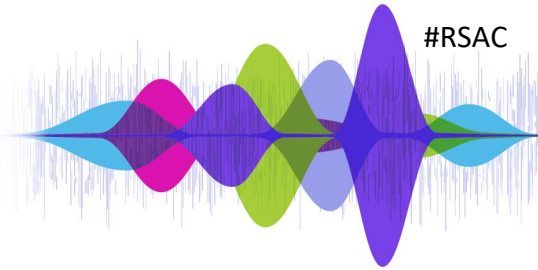
- **Actions Taken:**
  - **Stakeholder Engagement:** Identified risk areas and business pain points.
  - **Initiative Brainstorming:** Focused on preventing, detecting, and responding to security issues.
  - **Assessment & Prioritization:** Evaluated current security measures and prioritized high-impact, low-effort initiatives.
  - **Measurement & Optimization:** Established metrics and continuously refined processes.

Case Study #1 – The Beginning



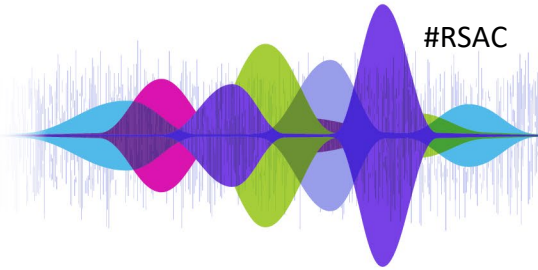
- **Results**:
  - Achieved 100% code coverage in vulnerability detection.
  - Met remediation Service Level Agreements (SLAs).
  - Introduced comprehensive security training, fostering a security-centric culture.

Case Study #2 – The Untrusted Ones



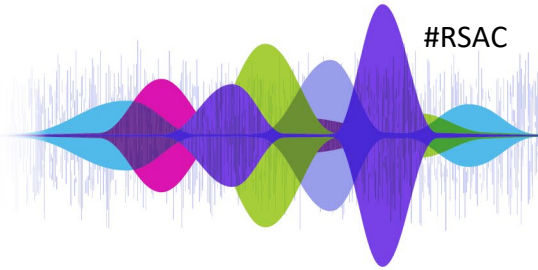
- **Challenge**:
  - AppSec team operated in isolation; lack of trust from developers.
  - Security seen as an obstacle; minimal collaboration.
- **Business Risk Tolerance:**
  - Medium—they could live with some risk but not cultural dysfunction.

Case Study #2 – The Untrusted Ones



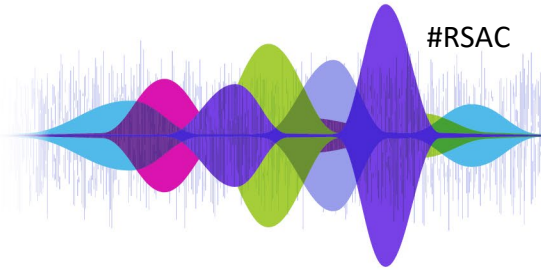
- **Actions Taken:**
  - **Relationship Building:** Opened dialogues with development teams to understand their perspectives.
  - **Collaborative Integration:** Embedded AppSec members within development teams for real-time support (now called “emissaries”).
  - **Process Improvement:** Streamlined security reviews and implemented automated tools for immediate feedback.
  - **Education & Empowerment:** Conducted tailored security training and established a Security Champions program.

Case Study #2 – The Untrusted Ones



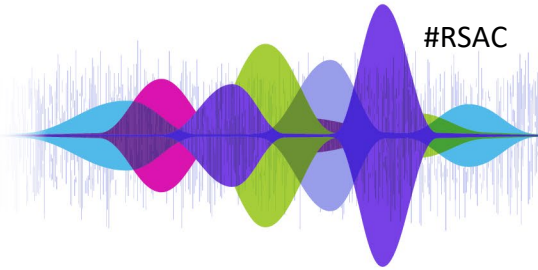
- **Results**
  - Enhanced trust and collaboration between AppSec and development teams.
  - Improved adherence to security recommendations, reducing vulnerabilities.
  - Cultivated a culture of shared security responsibility.

Case Study #3 – Ancient History



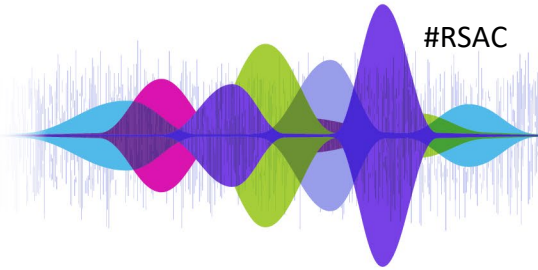
- **Challenge:**
  - Established AppSec team with outdated practices and no cohesive strategy.
  - Accumulated technical debt from obsolete security processes.
- **Business Risk Tolerance:**
  - High on paper, but unintentionally risky due to outdated processes.

Case Study #3 – Ancient History



- **Actions Taken:**
  - **Strategic Realignment:** Developed a clear AppSec strategy aligned with business objectives.
  - **Process Modernization:** Updated security policies and integrated modern practices into the SDLC.
  - **Continuous Improvement:** Established feedback loops to assess and refine security measures.
  - **Cultural Transformation:** Promoted proactive security mindsets and recognized contributions to security improvements.

Case Study #3 – Ancient History



- **Results:**
  - Reduced security-related technical debt.
  - Enhanced responsiveness to emerging security threats.
  - Developed a dynamic, strategic AppSec team aligned with organizational needs.

Case Study: What If…?

PREDICT	IDENTIFY	PREVENT		DETECT		RESPOND	
Threat Intelligence	M & A Security Playbook	Threat Modeling	AppSec Policies	SAST	SCA	Security SLA	Bug Bounty
AI Leveraging	NIST 800-53 Assessment	Security Champions	Team Self Development	DAST	MAST	External App Layer PenTests	PSIRT
Fraud Behavior	Internal Code Inventory	Metrics Dashboard	Security Architecture	Internal App PenTesting	Fuzzing	QA/AppSec Regression Testing	CTF Training
	ASVS Requirements	Dev Security Education	Vulnerability Guidelines	IAST	QA Partnership	Red Team Activities	Customer PenTests
	Asset Inventory	Vulnerability Remediation Education	Security Culture	CICD Integration	Validate 3rd Party APIs	WAF	Honey-potting
		Challenge Coin Award	Security Ambassadors	Container Scanning	Validate Partner Integrations	Typo-squatting Detection	Subdomain Validation
		Security Newsletter	Internal Security Summits	Security Test Code Coverage	Code Signing	Risk Acceptance	Reverse Engineering
		SSDLC Documentation	Monthly Brown Bags	Internal Security Toolkit	AppSecOps		
		QA Security Education	Enterprise Security Docs	Continuous Security Monitoring			
		Secure Coding Standards	Security Unit Tests				

NOT IMPLEMENTED
IMPLEMENTED
OPERATIONAL

Case Study: The Now

PREDICT	IDENTIFY	PREVENT		DETECT		RESPOND	
Threat Intelligence	M & A Security Playbook	Threat Modeling	AppSec Policies	SAST	SCA	Security SLA	Bug Bounty
AI Leveraging	NIST 800-53 Assessment	Security Champions	Team Self Development	DAST	MAST	External App Layer PenTests	PSIRT
Fraud Behavior	Internal Code Inventory	Metrics Dashboard	Security Architecture	Internal App PenTesting	Fuzzing	QA/AppSec Regression Testing	CTF Training
	ASVS Requirements	Dev Security Education	Vulnerability Guidelines	IAST	QA Partnership	Red Team Activities	Customer PenTests
	Asset Inventory	Vulnerability Remediation Education	Security Culture	CICD Integration	Validate 3rd Party APIs	WAF	Honey-potting
		Challenge Coin Award	Security Ambassadors	Container Scanning	Validate Partner Integrations	Typo-squatting Detection	Subdomain Validation
		Security Newsletter	Internal Security Summits	Security Test Code Coverage	Code Signing	Risk Acceptance	Reverse Engineering
		SSDLC Documentation	Monthly Brown Bags	Internal Security Toolkit	AppSecOps		
		QA Security Education	Enterprise Security Docs	Continuous Security Monitoring			
		Secure Coding Standards	Security Unit Tests				

NOT IMPLEMENTED

IMPLEMENTED

OPERATIONAL

Case Study: Year 1

PREDICT	IDENTIFY	PREVENT		DETECT		RESPOND	
Threat Intelligence	M & A Security Playbook	Threat Modeling	AppSec Policies	SAST	SCA	Security SLA	Bug Bounty
AI Leveraging	NIST 800-53 Assessment	Security Champions	Team Self Development	DAST	MAST	External App Layer PenTests	PSIRT
Fraud Behavior	Internal Code Inventory	Metrics Dashboard	Security Architecture	Internal App PenTesting	Fuzzing	QA/AppSec Regression Testing	CTF Training
	ASVS Requirements	Dev Security Education	Vulnerability Guidelines	IAST	QA Partnership	Red Team Activities	Customer PenTests
	Asset Inventory	Vulnerability Remediation Education	Security Culture	CICD Integration	Validate 3rd Party APIs	WAF	Honey-potting
		Challenge Coin Award	Security Ambassadors	Container Scanning	Validate Partner Integrations	Typo-squatting Detection	Subdomain Validation
		Security Newsletter	Internal Security Summits	Security Test Code Coverage	Code Signing	Risk Acceptance	Reverse Engineering
		SSDLC Documentation	Monthly Brown Bags	Internal Security Toolkit	AppSecOps		
		QA Security Education	Enterprise Security Docs	Continuous Security Monitoring			
		Secure Coding Standards	Security Unit Tests				

NOT IMPLEMENTED

IMPLEMENTED

OPERATIONAL

Case Study: Year 2 …and so forth

PREDICT	IDENTIFY	PREVENT		DETECT		RESPOND	
Threat Intelligence	M & A Security Playbook	Threat Modeling	AppSec Policies	SAST	SCA	Security SLA	Bug Bounty
AI Leveraging	NIST 800-53 Assessment	Security Champions	Team Self Development	DAST	MAST	External App Layer PenTests	PSIRT
Fraud Behavior	Internal Code Inventory	Metrics Dashboard	Security Architecture	Internal App PenTesting	Fuzzing	QA/AppSec Regression Testing	CTF Training
	ASVS Requirements	Dev Security Education	Vulnerability Guidelines	IAST	QA Partnership	Red Team Activities	Customer PenTests
	Asset Inventory	Vulnerability Remediation Education	Security Culture	CICD Integration	Validate 3rd Party APIs	WAF	Honey-potting
		Challenge Coin Award	Security Ambassadors	Container Scanning	Validate Partner Integrations	Typo-squatting Detection	Subdomain Validation
		Security Newsletter	Internal Security Summits	Security Test Code Coverage	Code Signing	Risk Acceptance	Reverse Engineering
		SSDLC Documentation	Monthly Brown Bags	Internal Security Toolkit	AppSecOps		
		QA Security Education	Enterprise Security Docs	Continuous Security Monitoring			
		Secure Coding Standards	Security Unit Tests				

NOT IMPLEMENTED

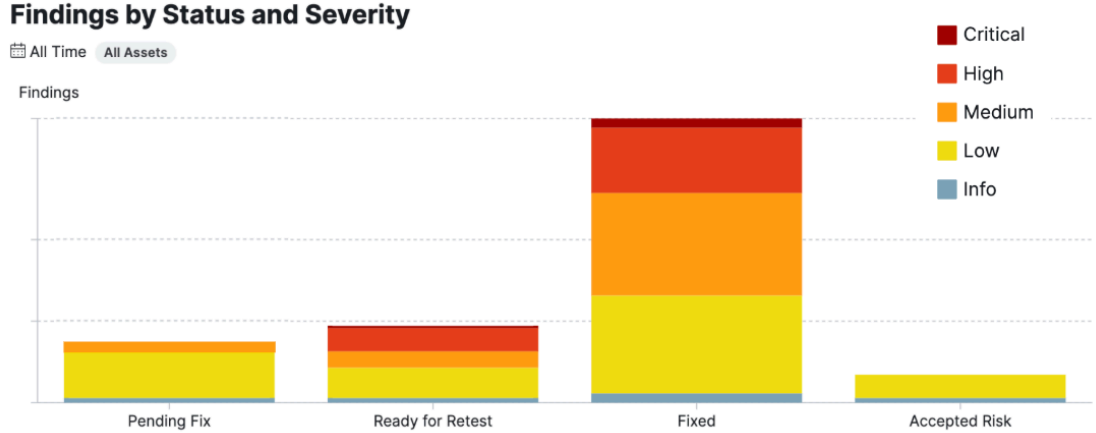
IMPLEMENTED

OPERATIONAL

An Operational Initiative MUST have impact on the Business AND Risk Posture

For example, with **External App Layer PenTesting**, operational does NOT mean all findings are addressed, but that there is a sustainable process, system, and organizational alignment to address findings.

What are other aspects of external PenTests that positively impact the security of the product?

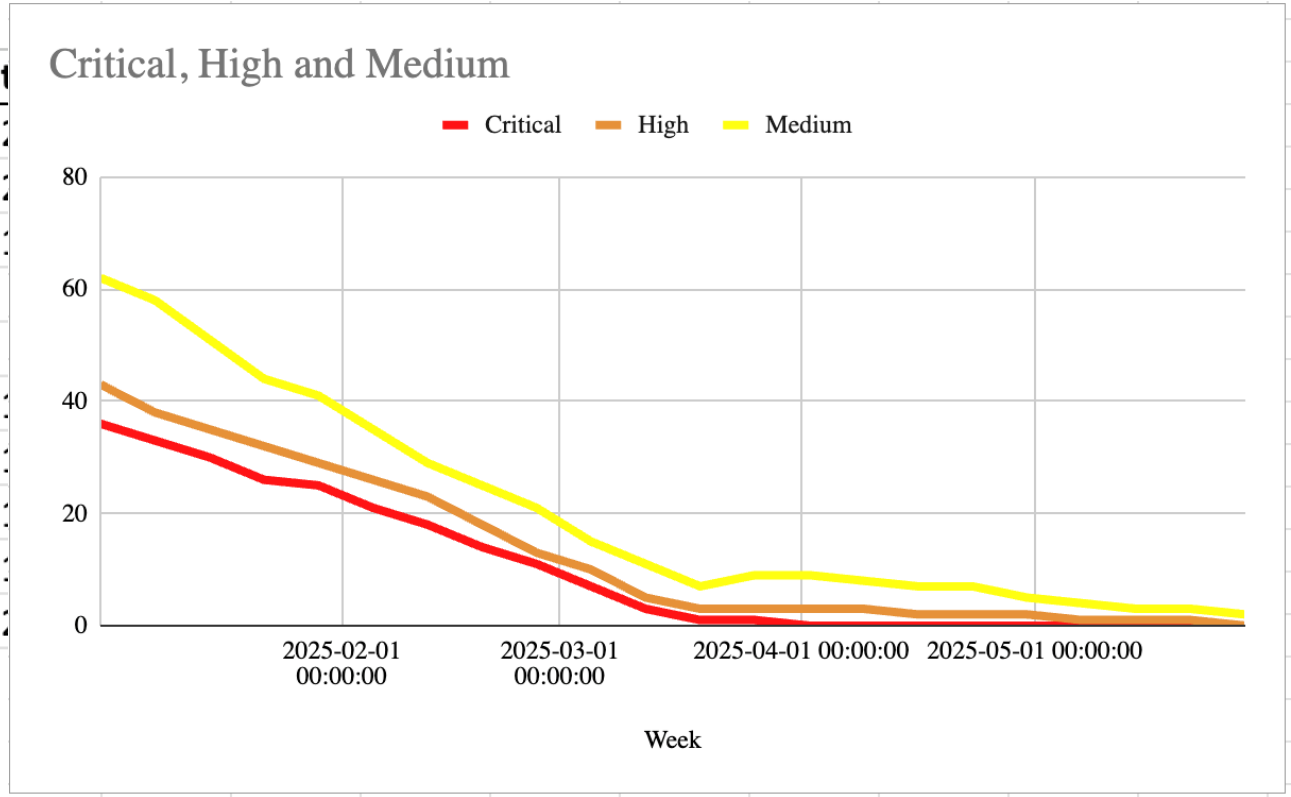


	Total Open	Open Vulns Outside of SLA			
		Critical	High	Medium	Low
Nordics	7	0	0	2	0
UK	2	0	0	0	0
USA	4	0	0	2	2
BeNeLux	3	0	0	0	3
DACH	5	0	0	1	4
ASEAN	3	0	0	0	3
Japan	1	0	0	0	1
ANZ	2	0	0	0	2
India	6	0	0	3	0

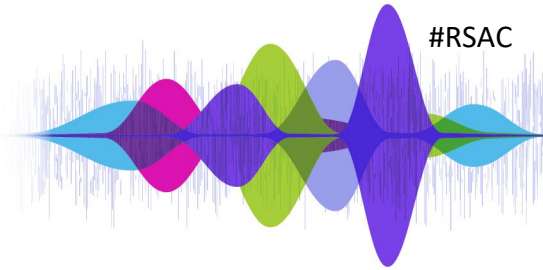
An Operational Initiative MUST have impact on the Business AND Risk Posture

Where there is operational focus with a collaborative approach, there must be positive improvements on risk posture. (Zero Out of SLA)

Line of Business	Critical Issues	Critical OOSLA	Avg Days OOSLA Crit
LOB 1	11	3	
LOB 2	8	7	
LOB 3	17	8	
LOB 4	19	5	
LOB 5	15	4	
LOB 6	12	8	
LOB 7	17	8	
LOB 8	9	3	
LOB 9	11	6	
LOB 10	14	5	



What You Can Do Now With Today's Info?



- **Build or expand your initiative list**: Use the supplied spreadsheet.
- **Assess where you are today**: Use the Not Implemented, Implemented, Operational model.
- **Interview key stakeholders**: Identify AppSec pain points.
- **Pick 1-2 high-impact initiatives**: Start small but meaningful.
- **Measure & refine**: Track progress on a regular basis.
- **Get executive buy-in**: Show how security reduces business risk.

RSAC 2025 Conference

Q & A

https://www.linkedin.com/in/kosorok/

Many Voices.
One Community.